



# Confident Solutions

## Autoryzowanie płatności



Dr Bartosz Wyżykowski  
radca prawny, partner  
bartosz.wyzykowski@dlklegal.com

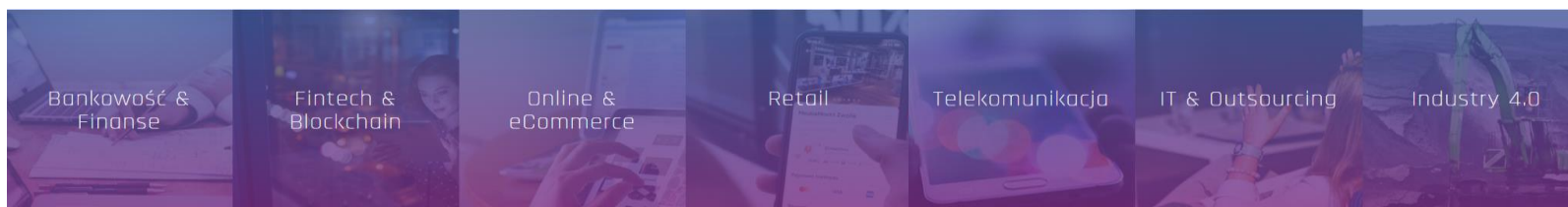
DLK LEGAL KORUS sp.k.  
www.dlklegal.com  
office@dlklegal.com  
Biura: Warszawa, Kraków

Teraźniejszość i przyszłość usług  
płatniczych - praktyczne wyzwania  
i nadchodzące regulacje  
MMC Polska, 17.06.2024 r.

Rozpowszechnianie wyłącznie za zgodą DLK Legal. Materiał ma charakter wyłącznie informacyjny - nie stanowi porady prawnej.

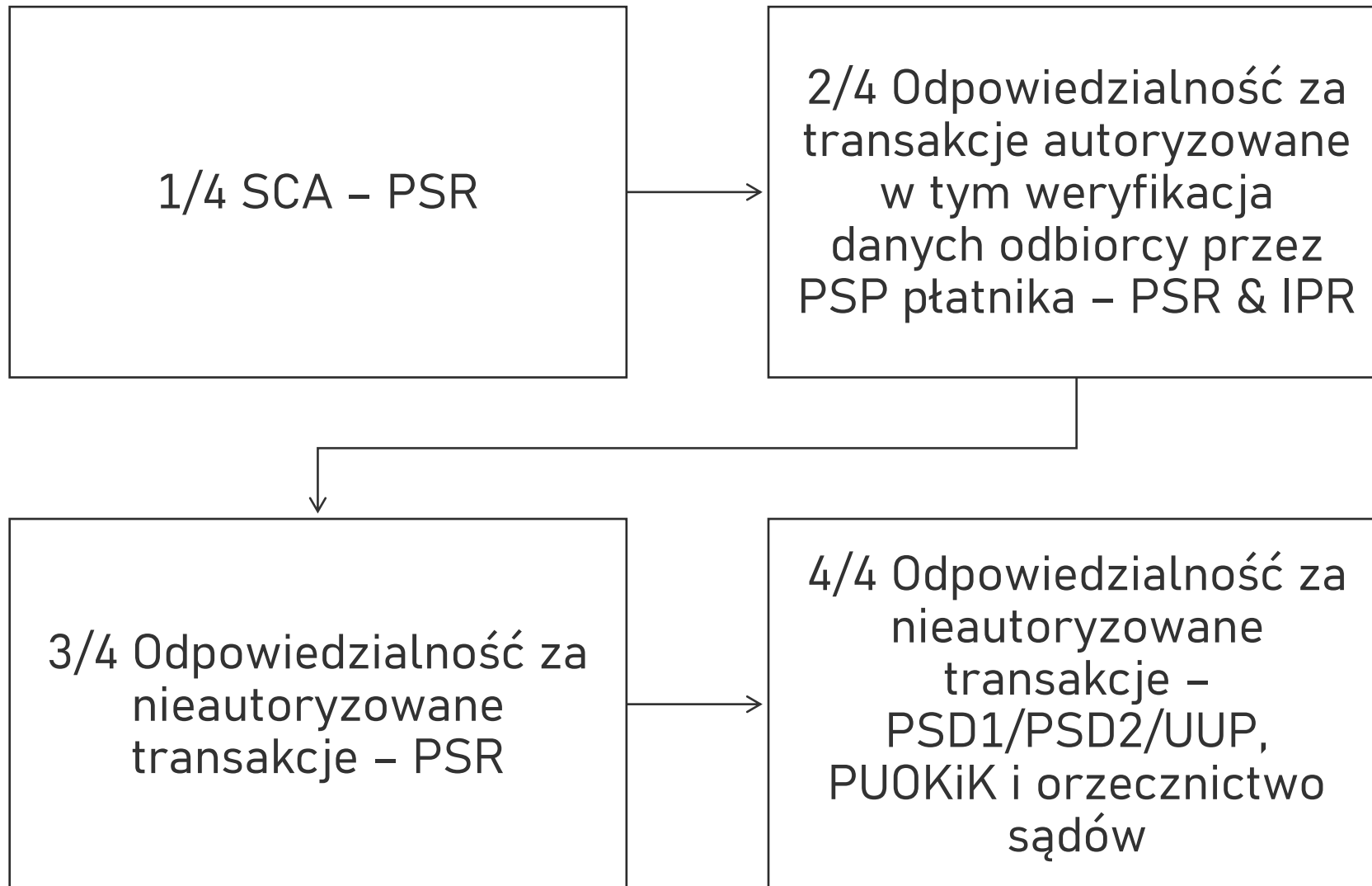
# „They are always able to provide confident solutions.” (Chambers 2020)

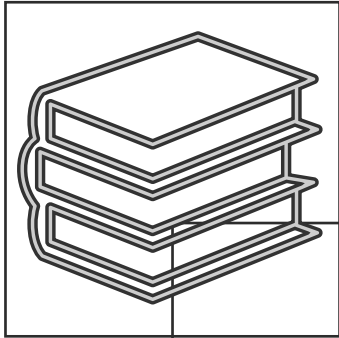
Wspieramy niezawodnie najbardziej innowacyjne sektory gospodarki w kluczowych procesach gospodarczych.



Regulacje +	Współpraca i Kontrakty B2B +	Environmental - Social - Governance (ESG) +
Transakcje - Inwestycje - Przekształcenia +	Finansowanie +	Obsługa bieżąca +
Spory i kontrowersje +	Nowe prawo i legislacja +	Kompetencje wewnętrzne +

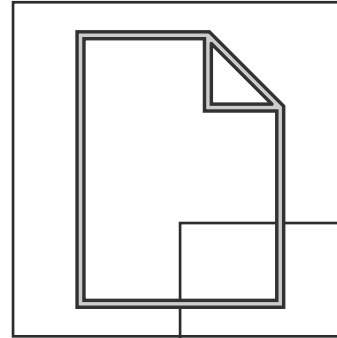
# Agenda





### PSR/PSD3

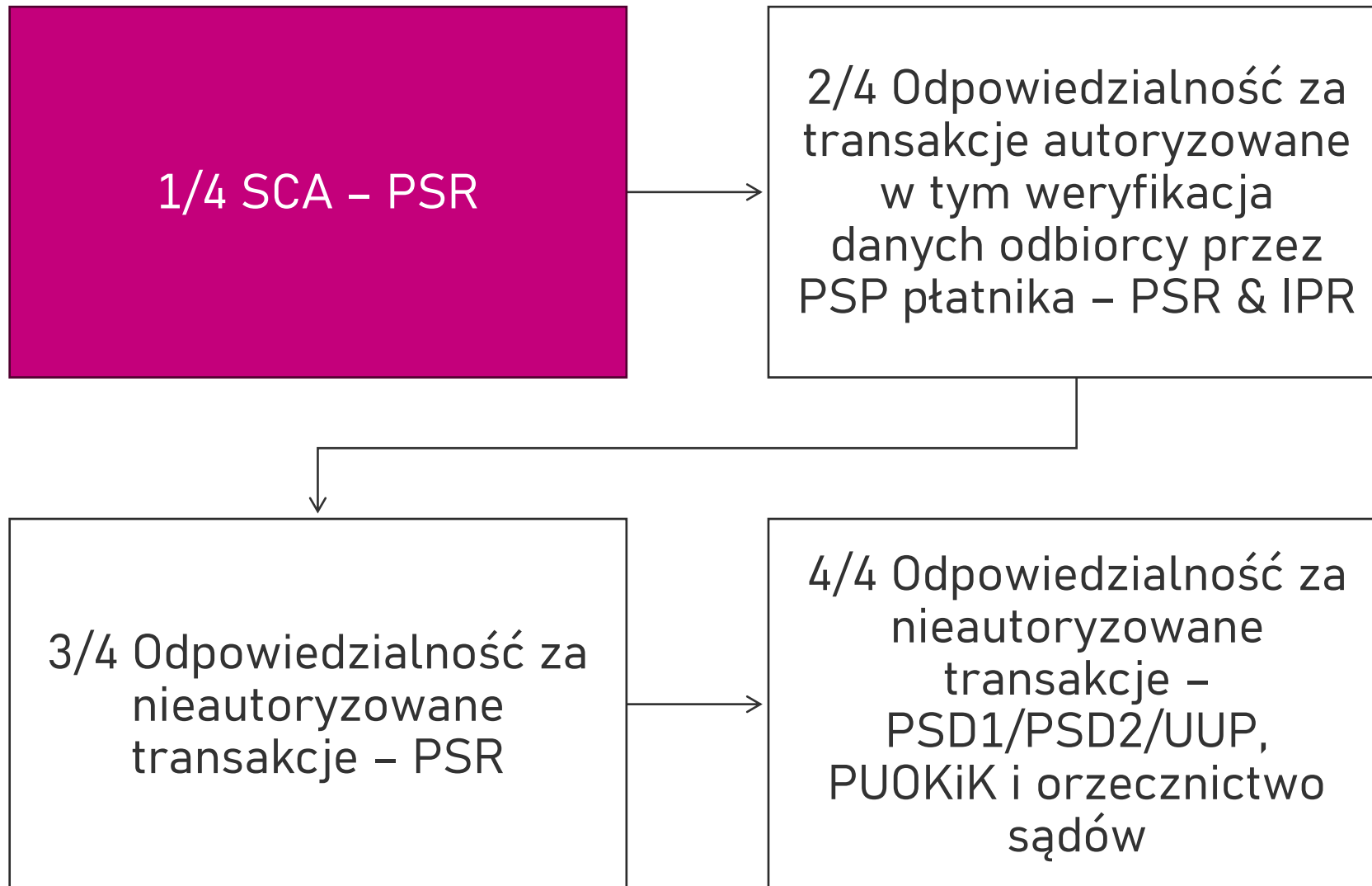
- Akty przyjęte w pierwszym czytaniu przez Parlament Europejski w dniu 23 kwietnia 2024 r.
- Akty będą przedmiotem prac w nowej kadencji PE



### IPR

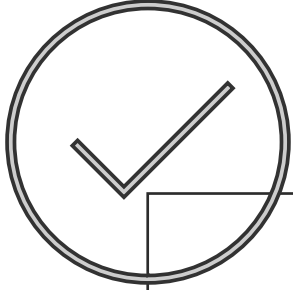
- Opublikowano w Dzienniku Urzędowym UE w dniu 19 marca 2024 r.

# Agenda



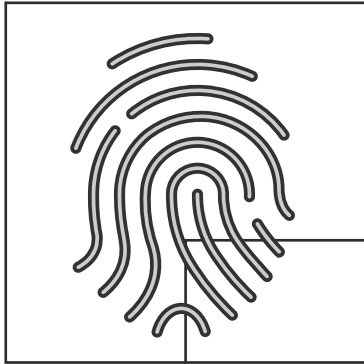
# SCA – PSR I 1b/9 Autoryzacja i uwierzytelnienie

	autoryzacja	uwierzytelnienie
co to:	klient zezwala na wykonanie transakcji płatniczej	dostawca upewnia się, że ma do czynienia ze swoim klientem
kiedy:	zlecenie transakcji	
		logowanie do rachunku
		inne czynności generujące ryzyko



## Elementy SCA

- SCA oznacza uwierzytelnianie w oparciu o zastosowanie co najmniej dwóch elementów należących do kategorii:
  - **wiedza** (coś, co wie wyłącznie użytkownik),
  - **posiadanie** (coś, co posiada wyłącznie użytkownik)
  - **cechy klienta** (coś, czym jest użytkownik), niezależnych w tym sensie, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnianie jest zaprojektowane w sposób zapewniający ochronę poufności danych uwierzytelniających.
- Nie jest konieczne, aby przynajmniej dwa elementy na których opiera się SCA, należały do różnych kategorii. Niezależność elementów jest zawsze w pełni zachowana, a procedura uwierzytelniania przez cały czas zapewnia wysoki poziom bezpieczeństwa.
- Element SCA „cechy klienta” może obejmować cechy środowiskowe i behawioralne, takie jak cechy związane z lokalizacją PSU, czas wykonania transakcji lub wykorzystywane urządzenie.



## Obowiązek stosowania SCA

- PSP płatnika stosuje SCA **opierając się na ocenie ryzyka przeprowadzonej w ramach mechanizmu monitorowania transakcji**, w przypadku gdy płatnik:
  - uzyskuje dostęp do swojego rachunku płatniczego w trybie online;
  - ~~uzyskuje dostęp do informacji o rachunku płatniczym;~~
  - składa zlecenie płatnicze dotyczące elektronicznej transakcji płatniczej;
  - przeprowadza czynność za pomocą kanału zdalnego, która może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć.
- Transakcje płatnicze niezainicjowane przez płatnika, ale przez odbiorcę, nie podlegają SCA wyłącznie w zakresie, w jakim transakcje te zainicjowano bez interakcji lub udziału płatnika. **Takie wyłączenia mają również zastosowanie do zwrotów inicjowanych przez pierwotnego odbiorcę na rzecz płatnika.**
- W tym celu PSP wprowadzają adekwatne środki bezpieczeństwa służące ochronie poufności i integralności indywidualnych danych uwierzytelniających użytkowników usług płatniczych.



# SCA – PSR I 5/9 Rozwiązania szczegółowe

## Papierowe zlecenia

Transakcje płatnicze, w przypadku których zlecenia płatnicze są składane przez płatnika w sposób inny niż przy użyciu platform lub urządzeń elektronicznych, takich jak **papierowe zlecenia płatnicze, zamówienia pocztowe** lub **mechanizmy oparte na telefonii** nie podlegają SCA, niezależnie od tego czy transakcja jest przeprowadzona drogą elektroniczną, pod warunkiem, że PSP płatnika spełnia wymogi i przeprowadza kontrole w zakresie bezpieczeństwa, które umożliwiają **inną formę uwierzytelniania** transakcji płatniczej niż **SCA**.

## Dynamiczne łączenie

W przypadku zdalnego złożenia zlecenia płatniczego dotyczącego **elektronicznej transakcji płatniczej**, PSP stosują SCA obejmujące elementy, które dynamicznie łączą transakcję z określoną kwotą i określonym odbiorcą.

## SCA +

## Technologia zbliżeniowa

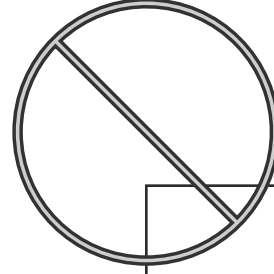
W przypadku złożenia zlecenia płatniczego dotyczącego **elektronicznej transakcji płatniczej**, składanego za pomocą urządzenia płatnika wykorzystującego **technologię zbliżeniową** do celów wymiany informacji z infrastrukturą odbiorcy, do celów uwierzytelnienia, którego wymaga **skorzystanie z internetu** na urządzeniu płatnika, PSP **stosują SCA**, które obejmuje elementy dynamicznie łączące transakcję z określoną kwotą i określonym odbiorcą **lub zharmonizowane środki bezpieczeństwa dające taki sam efekt, które to środki zapewniają poufność, autentyczność i integralność kwoty i odbiorcy transakcji we wszystkich fazach inicjowania**.

# SCA – PSR I 6/9 Nieautoryzowane transakcje



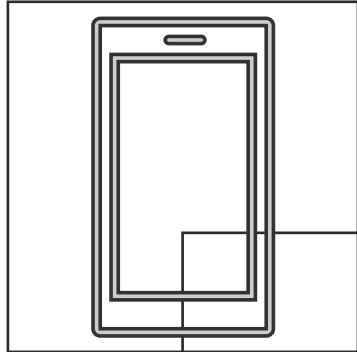
## Brak spełnienia obowiązku SCA

- W przypadku gdy PSP płatnika **nie spełnia obowiązku nałożenia wymogu SCA**, płatnik nie ponosi żadnych szkód finansowych, chyba że płatnik działał w złej wierze.
- Dotyczy to także sytuacji, w której PSP płatnika albo odbiorcy **stosuje wyłączenie ze stosowania SCA**.
- W przypadku gdy odbiorca lub PSP odbiorcy nie opracują lub nie zmienią systemów, sprzętu i oprogramowania niezbędnego do stosowania SCA, **odbiorca lub PSP odbiorcy** zwracają szkody finansowe wyrządzone PSP płatnika.



## Stosowanie wyłączenia SCA

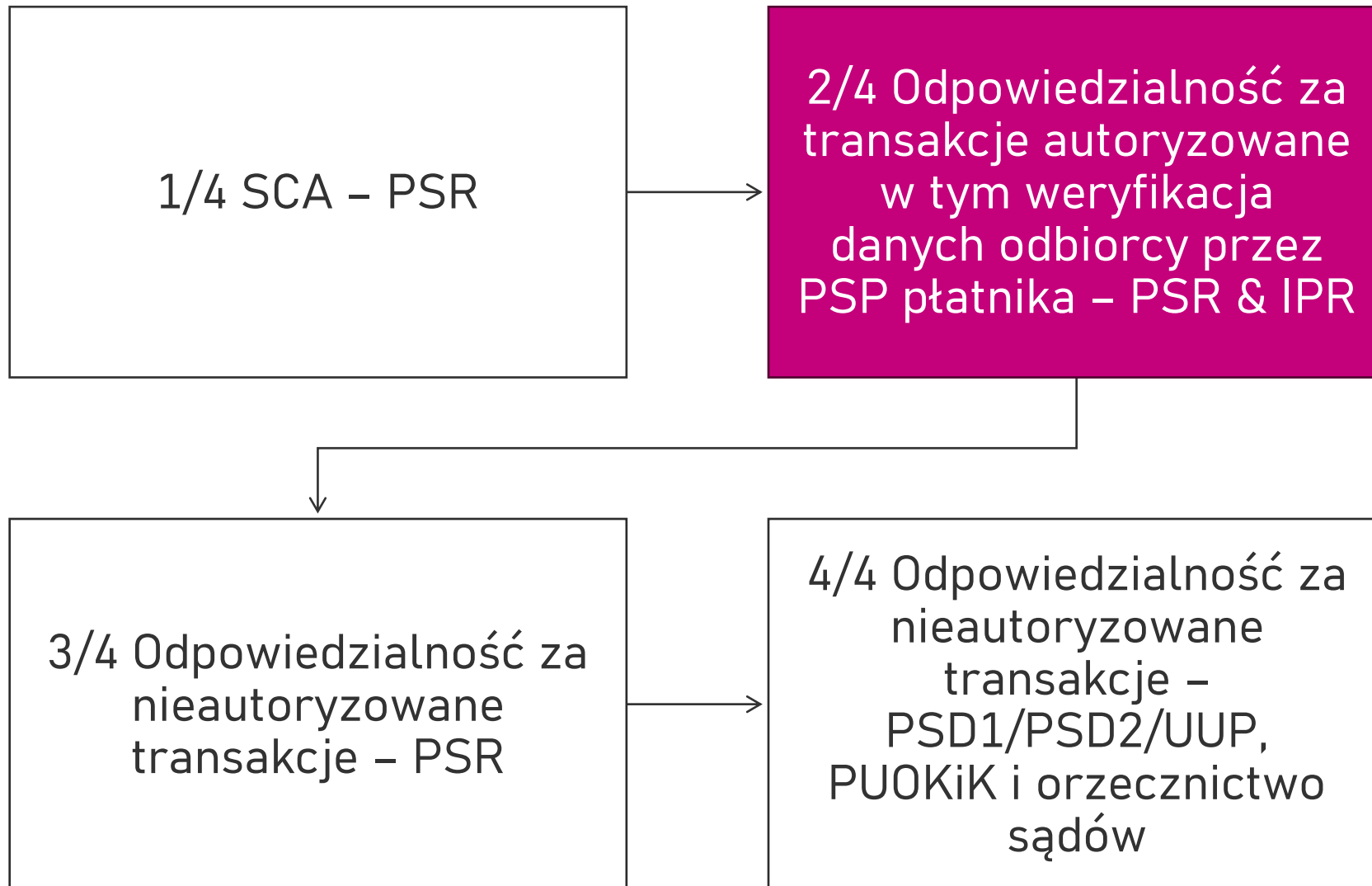
- W przypadku gdy **PSP odbiorcy stosuje wyłączenie ze stosowania SCA**, PSP odbiorcy ponosi **odpowiedzialność wobec PSP płatnika** za wszelkie szkody finansowe poniesione przez płatnika.

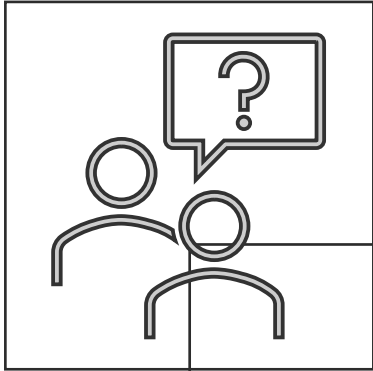


## Inkluzywność

- Bez uszczerbku dla wymogów dostępności określonych w dyrektywie 2019/882, PSP zapewniają, by **wszyscy ich klienci, w tym osoby z niepełnosprawnościami, osoby starsze, osoby posiadające niewielkie umiejętności cyfrowe oraz nieposiadające dostępu do kanałów cyfrowych lub instrumentów płatniczych, miały do dyspozycji co najmniej jeden środek, dostosowany do ich szczególnych potrzeb, umożliwiający im przeprowadzenie SCA.**
- PSP nie mogą uzależniać przeprowadzania SCA, **które ma być świadczone bezpłatnie**, od wyłącznego korzystania z jednego sposobu uwierzytelniania i **nie mogą uzależnić, w sposób wyraźny lub dorozumiany**, przeprowadzania SCA od posiadania smartfona **lub innego inteligentnego urządzenia**. PSP opracowują **więcej niż jeden sposób** stosowania SCA, aby zadbać o **różne szczególne potrzeby wszystkich swoich klientów, w szczególności osób z niepełnosprawnościami, osób posiadających niewielkie umiejętności cyfrowe, osób starszych i osób nieposiadających dostępu do kanałów cyfrowych lub instrumentów płatniczych.**

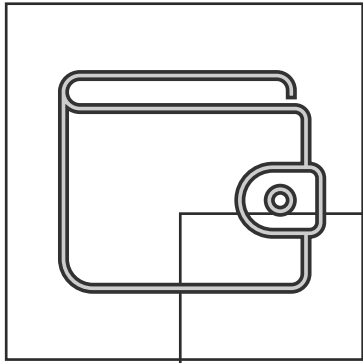
# Agenda





## Usługa weryfikacji dopasowania

- Obowiązek świadczenia **bezpłatnej** usługi weryfikacji dopasowania (nazwiska/nazwy oraz unikatowego identyfikatora).
- Dotyczy **poleceń przelewu**.
- PSP odbiorcy bezpłatnie weryfikuje na wniosek PSP płatnika czy unikatowy identyfikator i nazwisko/nazwa są dopasowane i **powiadamia o wyniku** PSP płatnika.
- Usługa świadczona niezwłocznie po podaniu przez płatnika unikatowego identyfikatora odbiorcy oraz nazwiska/nazwy odbiorcy, a przed zaoferowaniem możliwości autoryzacji
- Jeżeli brak dopasowania, PSP płatnika powiadamia płatnika **o rozbieżności i jej stopniu**.
- Dotyczy zleceń płatniczych złożonych za pośrednictwem **elektronicznych kanałów** inicjowania płatności oraz za pośrednictwem zleceń płatniczych **innych niż elektroniczne**, obejmujących interakcję **w czasie rzeczywistym** pomiędzy płatnikiem a PSP płatnika.
- Usługa nie jest wymagana, jeżeli płatnik sam nie podał unikatowego identyfikatora ani nazwiska lub nazwy odbiorcy.



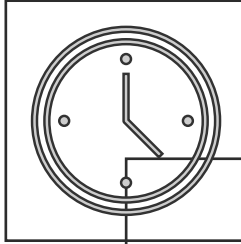
## Odpowiedzialność na gruncie IPR

- Dostawca usług płatniczych **nie ponosi odpowiedzialności za wykonanie polecenia przelewu na rzecz niezamierzonego odbiorcy na podstawie nieprawidłowego unikatowego identyfikatora**,
- W przypadku gdy PSP płatnika nie zaoferuje płatnikowi usługi polegającej na zapewnieniu weryfikacji odbiorcy, na rzecz którego płatnik zamierza wykonać polecenie przelewu lub nie zapewni prawidłowości informacji dotyczących odbiorcy przy inicjowaniu płatności, gdy identyfikator rachunku płatniczego lub nazwa odbiorcy są podane przez dostawcę świadczącego usługę inicjowania płatności, a nie przez płatnika i jeżeli skutkuje to wadliwie wykonaną transakcją płatniczą, **PSP płatnika bezzwłocznie zwraca płatnikowi transferowaną kwotę i, w stosownych przypadkach, przywraca obciążony rachunek płatniczy do stanu, jaki istniałby, gdyby transakcja nie miała miejsca.**
- W przypadku gdy uchybienie takie ma miejsce, ponieważ PSP odbiorcy lub dostawca świadczący usługę inicjowania płatności nie dopełnili swoich obowiązków w tym zakresie, PSP odbiorcy lub, w stosownych przypadkach, dostawca świadczący usługę inicjowania **płatności rekompensują PSP płatnika szkodę finansową wyrządzoną dostawcy usług płatniczych płatnika w wyniku tego uchybienia.**
- Wszelkie dalsze straty finansowe wyrządzone płatnikowi **mogą zostać zrekompensowane zgodnie z prawem mającym zastosowanie do umowy między płatnikiem a stosownym PSP.**



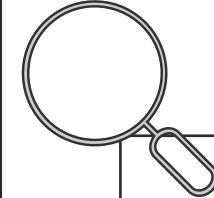
## Rozszerzona odpowiedzialność

- użytkownik będący **konsumentem**
- uległ manipulacji osoby trzeciej udającej pracownika PSP konsumenta **lub jakkolwiek inny właściwy podmiot publiczny lub prywatny,**
- bezprawnie wykorzystującej nazwisko lub nazwę bądź adres e-mail lub numer telefonu tego PSP/**podmiotu,**
- doszło do nielegalnych **autoryzowanych** transakcji płatniczych,
- PSP zwróci konsumentowi pełną kwotę nielegalnej autoryzowanej transakcji płatniczej pod warunkiem, że konsument niezwłocznie zgłosił **oszustwo policji oraz powiadomił PSP.**



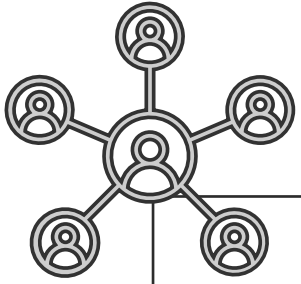
## Konsekwencje

- W terminie 10 dni roboczych po odnotowaniu nielegalnej autoryzowanej transakcji płatniczej, po otrzymaniu stosownego zgłoszenia **lub raportu z policji** PSP podejmuje jedno z następujących działań:
  - dokonuje na rzecz konsumenta zwrotu kwoty nielegalnej autoryzowanej transakcji płatniczej
  - jeżeli PSP ma uzasadnione podstawy, aby podejrzewać, że konsument popełnił **oszustwo lub dopuścił się rażącego niedbalstwa,** przekazuje **organowi krajowemu merytoryczne** uzasadnienie odmowy dokonania zwrotu i wskazuje organy, do których konsument może skierować sprawę jeżeli konsument nie zgadza się z przedstawionym uzasadnieniem.



## Wyłączenie i ciężar dowodu

- Nie stosuje się gdy konsument działał w nieuczciwych zamiarach, dopuścił się rażącego niedbalstwa, **odmawia udziału w dochodzeniu PSP lub dostarczenia informacji dot. podszywania się**
- Ciężar udowodnienia, że konsument działał w nieuczciwych zamiarach lub dopuścił się rażącego niedbalstwa, spoczywa na PSP konsumenta.



## Odpowiedzialność platformy

- Do wzrostu liczby oszustw mogą również przyczyniać się platformy internetowe. W związku z tym, bez uszczerbku dla ich obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 (akt o usługach cyfrowych), powinni oni zostać pociągnięci do odpowiedzialności w przypadku, gdy oszustwa powstały bezpośrednio w wyniku wykorzystania przez oszustów ich platformy do oszukania konsumentów, jeżeli zostali poinformowani o oszukańczych treściach znajdujących się na ich platformie i nie usunęli ich.
- Przepisy art. 59 mają również zastosowanie do dostawców usług łączności elektronicznej i platform internetowych.

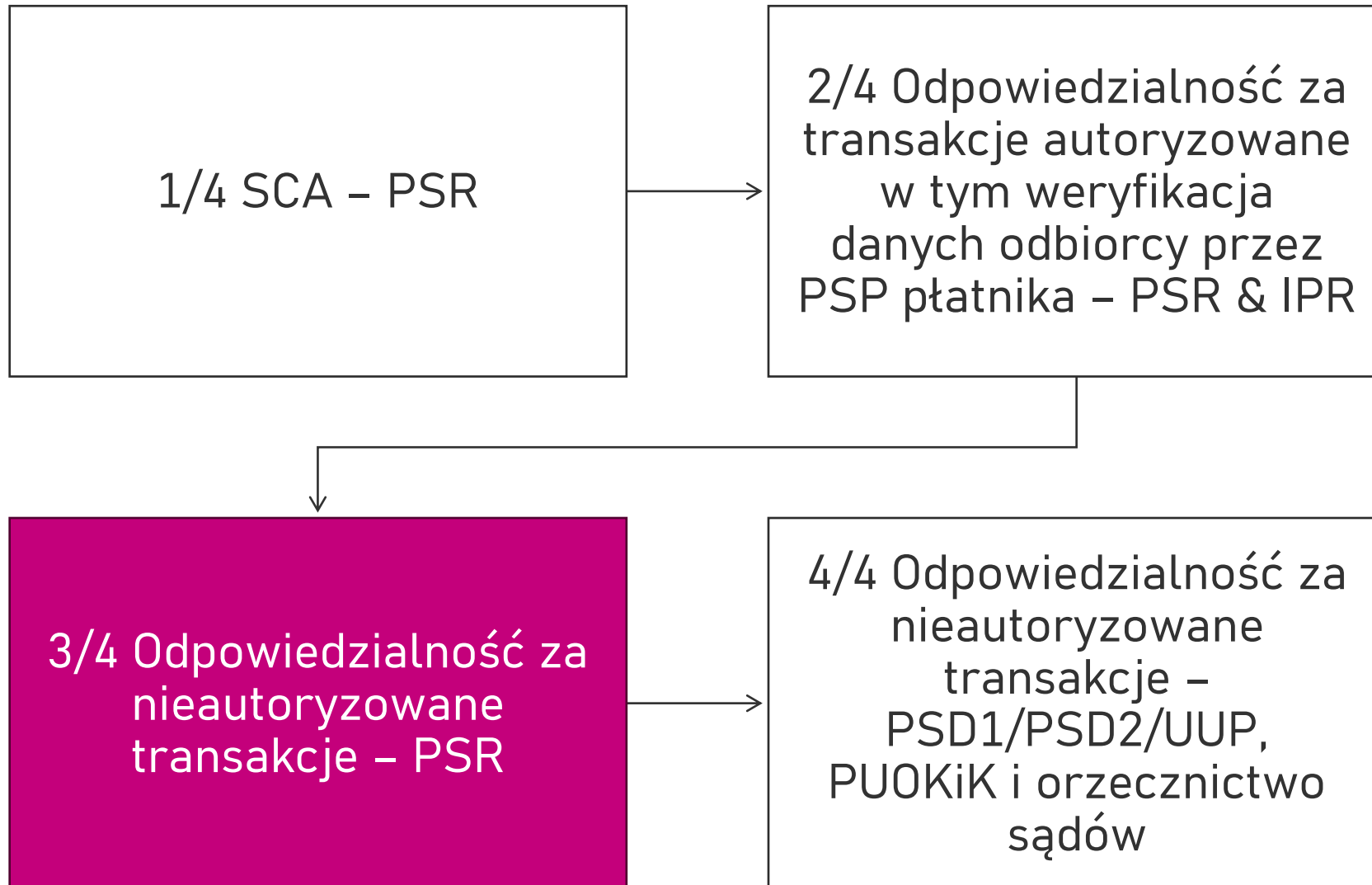


## Platforma czy telekom?

- Jeżeli **dostawcy usług łączności elektronicznej** nie usuną oszukańczych lub nielegalnych treści, po otrzymaniu informacji o ich wystąpieniu, zwracają dostawcy usług płatniczych pełną kwotę nielegalnej autoryzowanej transakcji płatniczej, pod warunkiem że konsument niezwłocznie zgłosił oszustwo policji i powiadomił o tym swojego dostawcę usług płatniczych.
- **Dostawcy usług łączności elektronicznej** wprowadzają wszelkie niezbędne środki edukacyjne, w tym ostrzeżenia dla swoich klientów za pośrednictwem wszelkich odpowiednich środków i mediów w przypadku pojawienia się nowych form oszustw internetowych, z uwzględnieniem potrzeb najbardziej bezbronnych grup klientów



# Agenda





## Zgoda - PSD2

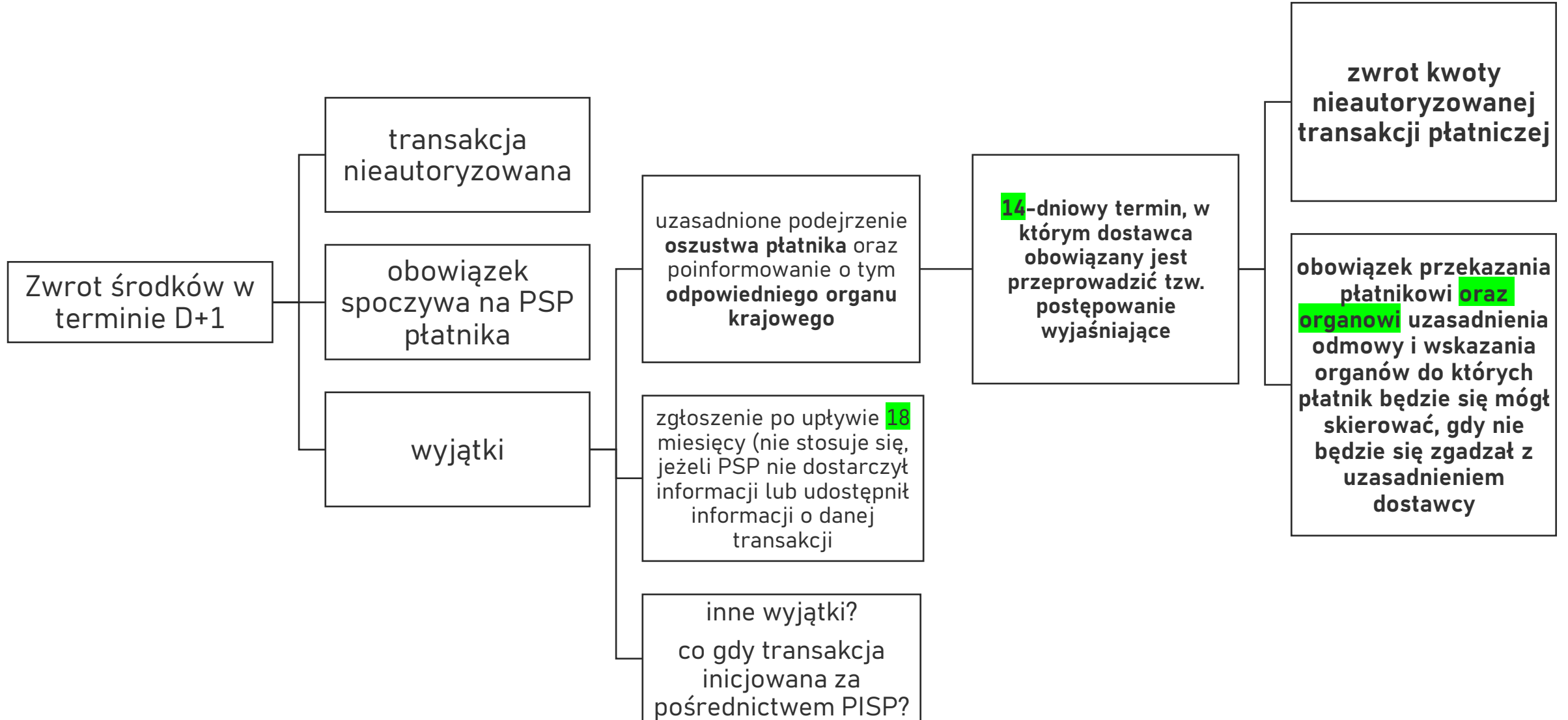
- Państwa członkowskie zapewniają, aby transakcję płatniczą uznawano za autoryzowaną tylko **pod warunkiem udzielenia przez płatnika zgody na wykonanie transakcji płatniczej**



## Zezwolenie - PSR

- Transakcja płatnicza lub kilka transakcji płatniczych mogą być autoryzowane wyłącznie wówczas, **gdy płatnik udzielił zezwolenia na wykonanie transakcji płatniczej**

# Odpowiedzialność za transakcje nieautoryzowane | 2/5 Obowiązek zwrotu D + 1



# Odpowiedzialność za transakcje nieautoryzowane | 3/5 Odpowiedzialność

## podział odpowiedzialności z tytułu nieautoryzowanej transakcji płatniczej

Art. 60 ust. 1 *in fine* PSR

W przypadku gdy płatnik nie działał w nieuczciwych zamiarach ani nie zaniedbał celowo swoich obowiązków, o których mowa w art. 52, **właściwe organy krajowe lub dostawcy usług płatniczych** mogą ograniczyć odpowiedzialność, biorąc pod uwagę w szczególności charakter indywidualnych danych uwierzytelniających oraz konkretne okoliczności, w których dany instrument płatniczy został utracony, skradziony lub przywłaszczony.

### płatnik

do 50 EUR jeżeli:

- nieautoryzowana transakcja jest skutkiem
  - 1) postużenia się utraconym przez płatnika lub
  - 2) skradzionym płatnikowi instrumentem płatniczym lub
  - 3) przywłaszczenia instrumentu płatniczego
- działał w nieuczciwych zamiarach
- albo działając w nieuczciwych zamiarach lub dopuszczając się celowego lub rażącego zaniedbania obowiązków ostrożnościowych o których mowa w art. 52 PSR

w pełnej wysokości - jeśli płatnik

### dostawca

- w pełnej wysokości

płatnik nie miał możliwości stwierdzenia utraty, kradzieży przywłaszczenia instrumentu płatniczego **lub danych uwierzytelniających** (chyba, że nieuczciwe zamiary płatnika)

brak stosowania SCA

przyczyna stronie dostawcy (pracownik, oddział, agent, lub insourcer)

Obowiązki ostrożnościowe

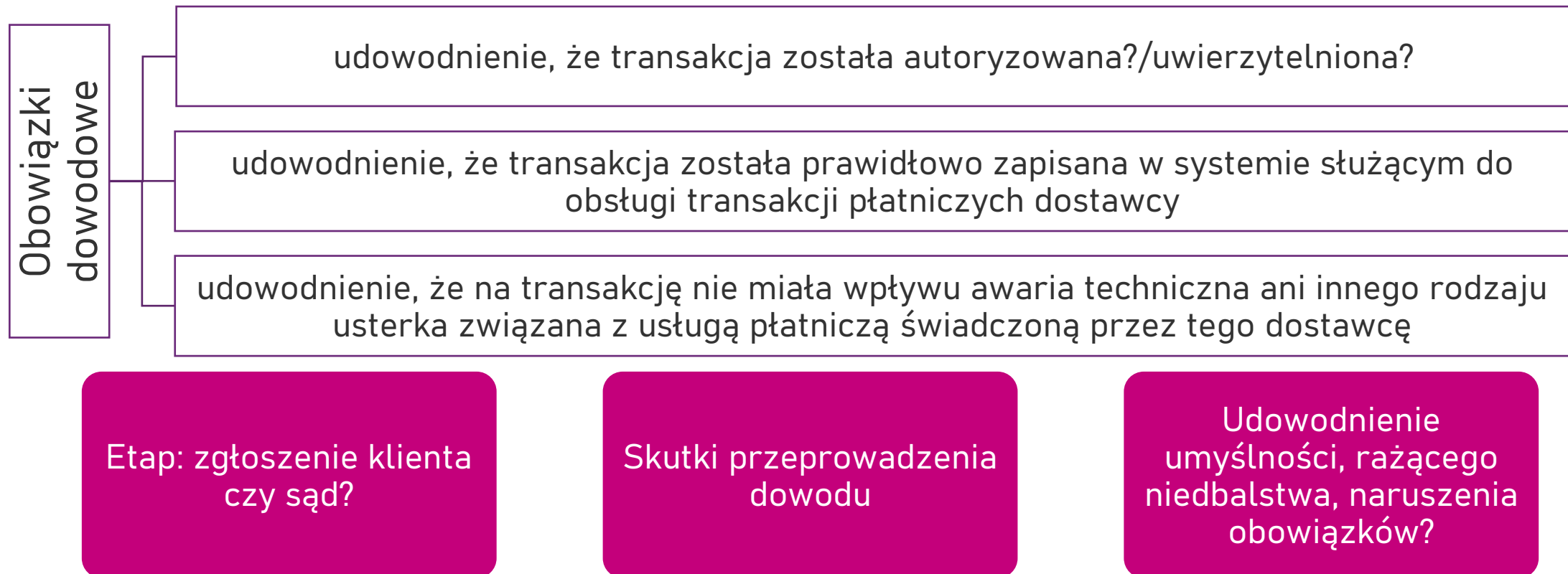
postępowanie zgodnie z umową

bezpieczne przechowywanie instrumentu płatniczego

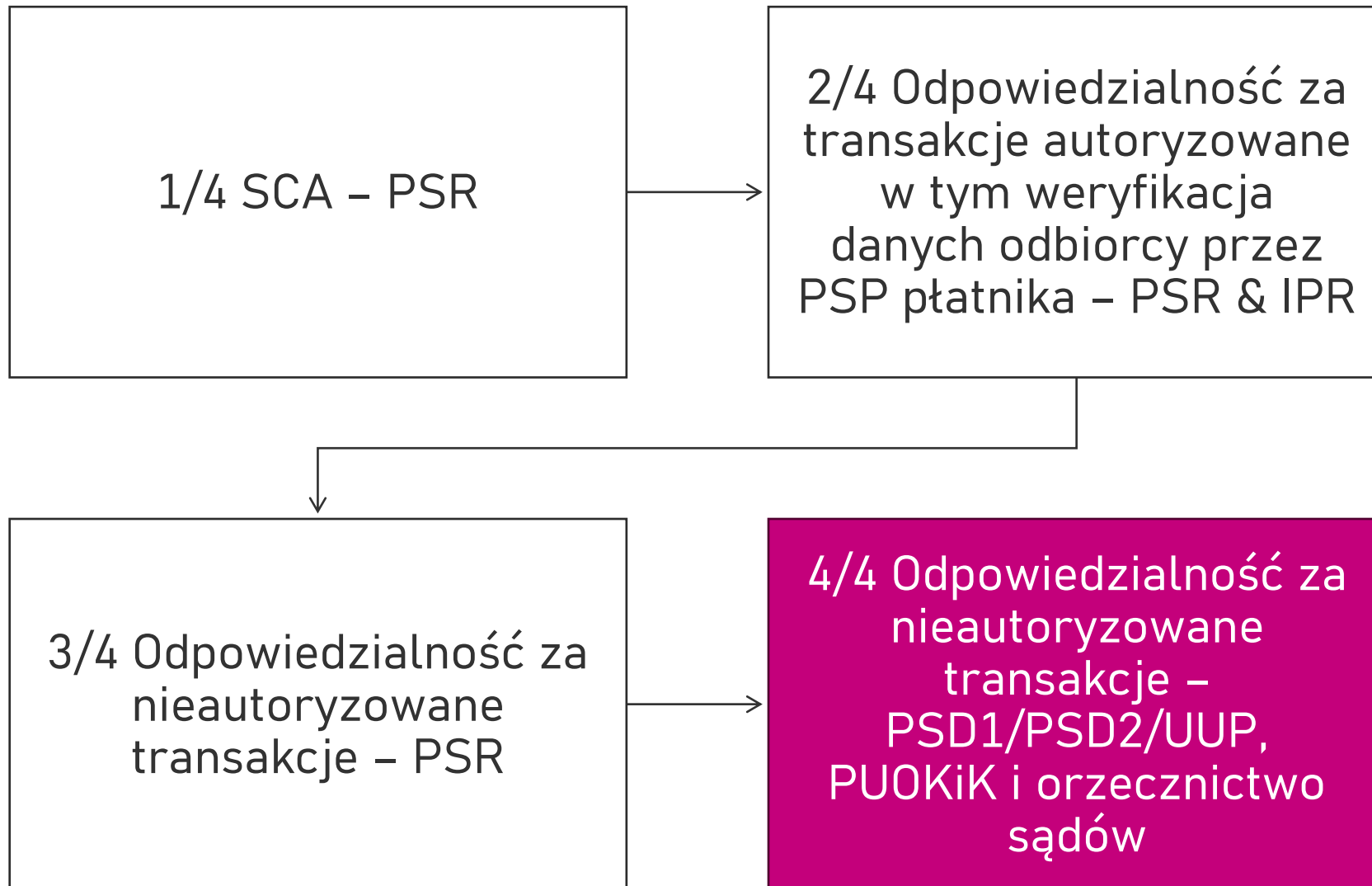
niezwłoczne dokonanie zgłoszenia utraty

# Odpowiedzialność za transakcje nieautoryzowane | 4a/5 Ciężary dowodowe

- Ogólna zasada:
  - ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne
  - strony są obowiązane wskazywać dowody dla stwierdzenia faktów, z których wywodzą skutki prawne
- UUP w ślad za PSD2 wprowadza wyjątki:



# Agenda



# Odpowiedzialność za transakcje nieautoryzowane 2024 | 1/7 Stan obecny



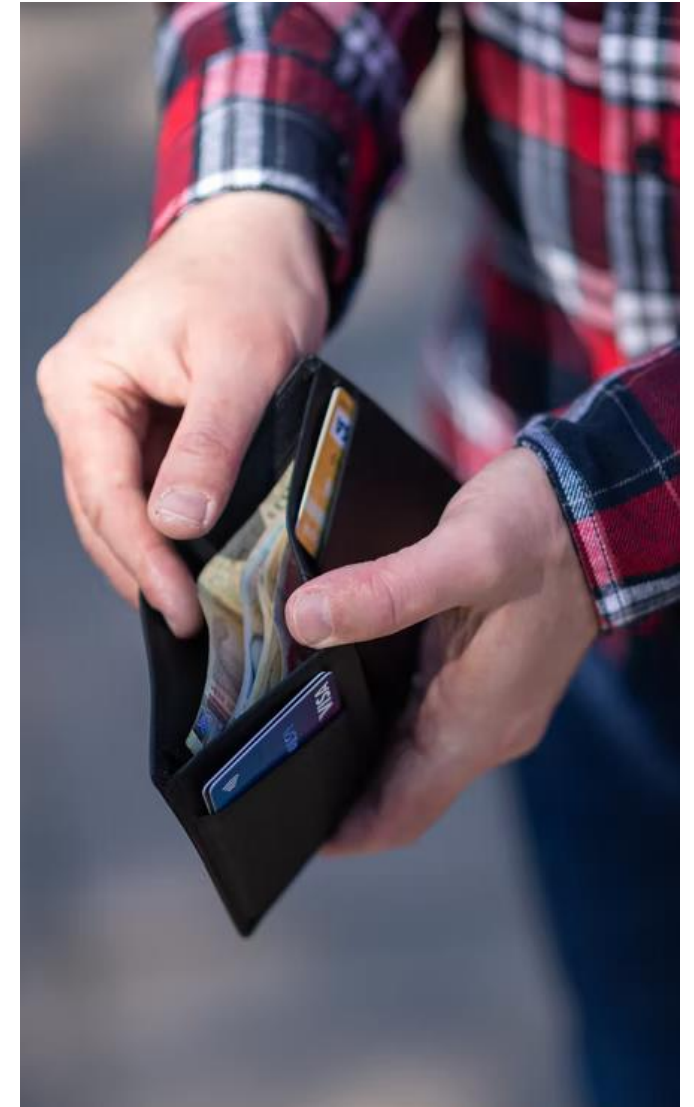
## Postępowania UOKiK przeciwko bankom

- Lipiec 2021: postępowania wyjaśniające (18 banków)
- Lipiec 2022: postępowania w sprawie ZIK (5 banków)
- Zarzuty dotyczą:
  - bezprawnej odmowy zwrotu kwoty nieautoryzowanych transakcji
  - wprowadzania konsumentów w błąd w odpowiedziach na reklamacje



## Projekt nowelizacji UUP (UD 52)

- Częściowe usunięcie błędów implementacji PSD1/PSD2
- Osobista autoryzacja transakcji przez użytkownika
- Ostatnia aktualizacja projektu w RCL: 30-09-2022



# Odpowiedzialność za transakcje nieautoryzowane 2024 | 2/7 Sekwencja działań

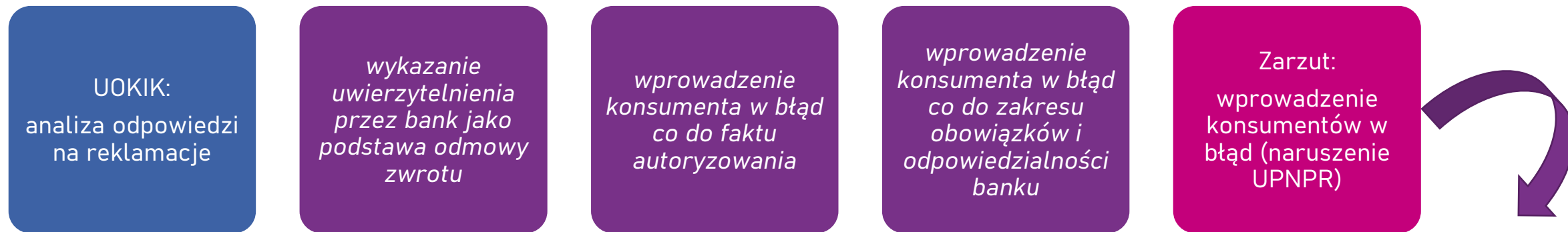
Prezes UOKiK

- *Dopiero po wypełnieniu obowiązku zwrotu bank może dochodzić roszczeń od klienta, jeśli okaże się, że klient doprowadził do transakcji umyślnie albo wykazał się rażącym niedbalstwem, umożliwiając oszustom wykorzystanie jego danych uwierzytelniających. Ciężar wykazania tych okoliczności, zgodnie z prawem, spoczywa na banku.*

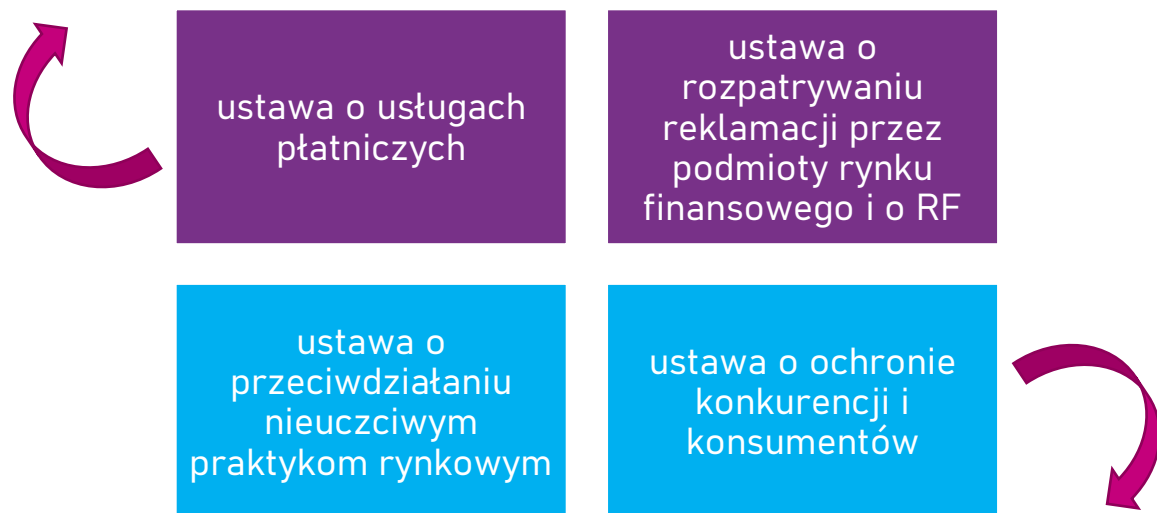




# Odpowiedzialność za transakcje nieautoryzowane 2024 | 3/7 Zarzuty Prezesa UOKiK



**przepisy materialne**  
(w przypadku konsumentów zakaz wyłączenia)



**przepisy ustrojowe**

Tu jesteś: Strona główna > Urząd > Informacje ogólne > Aktualności

## Transakcje nieautoryzowane - zarzuty wobec 5 banków

podziel się

18.07.2022 < poprzedni | następny >

**TRANSAKcje NIEAUTORYZOWANE**

- > Z konta bez twojej zgody zniknęły pieniądze, zgłosiłeś to do banku, a ten odmówił zwrotu kwoty nieautoryzowanej transakcji?
- > Zgodnie z prawem na banku spoczywa odpowiedzialność dochowania szczególnej staranności w zakresie przechowywania i ochrony środków pieniężnych.
- > Bank musi zwrócić konsumentowi pieniądze, chyba że podejrzewa oszustwo z jego strony i zawiadomił o tym organy ścigania.
- > Prezes UOKiK postawił zarzuty 5 bankom - dotyczą bezprawnej odmowy zwrotu kwoty nieautoryzowanych transakcji i wprowadzania konsumentów w błąd w odpowiedziach na reklamacje.

Prezes UOKiK od roku prowadzi [postępowania wyjaśniające w sprawie nieautoryzowanych transakcji](#). Zebrany do tej pory materiał dowodowy pozwolił obecnie postawić 5 bankom zarzuty naruszania zbiorowych interesów konsumentów. Są to: **Bank Millennium, BNP Paribas Bank Polska, Credit Agricole Bank Polska, mBank oraz Santander Bank Polska.**



# Confident Solutions

Q&A



Dr Bartosz Wyżykowski  
radca prawny, partner  
bartosz.wyzykowski@dlklegal.com

DLK LEGAL KORUS sp.k.  
www.dlklegal.com  
office@dlklegal.com  
Biura: Warszawa, Kraków

Teraźniejszość i przyszłość usług  
płatniczych - praktyczne wyzwania  
i nadchodzące regulacje  
MMC Polska, 17.06.2024 r.

Rozpowszechnianie wyłącznie za zgodą DLK Legal. Materiał ma charakter wyłącznie informacyjny - nie stanowi porady prawnej.